Block compromised devices: AT&T Managed Endpoint Security with SentinelOne – Ranger

Find and control what's on your network with our endpoint security solution

Modern cyberattacks have become highly sophisticated. Adversaries look for vulnerabilities in your defenses to infiltrate your business network and wreak havoc. Anything connected to your network—a printer, kiosk device, or digital signage—can become home base for the hacker to conduct their reconnaissance missions and move laterally within the network to advance their attack.

The speed and scale of newly connected devices compound these vulnerabilities. The proliferation of the Internet of Things (IoT) in business, open BYOD policies, and a global remote workforce has exponentially increased the number of unmanaged IP-enabled devices that may be on your company's network. Cyberattackers are using this explosion in IP-enabled devices to find new ways to infiltrate a business.

AT&T Managed Endpoint Security with SentinelOne – Ranger can help gain visibility and control over what is on your network. Ranger is an add-on service to AT&T Managed Endpoint Security with SentinelOne. You enableit through the same SentinelOne agent on the endpoint. Administrators have the flexibility to specify a different policy for each network and subnet if needed.

Count on award-winning cybersecurity

Features

- 1-click network visibility and control over unknown and IoT network devices
- Machine learning device fingerprinting via active and passive scanning
- Highly configurable per subnet
- No added software, hardware, or network changes

Benefits

- Discover unknown devices and create alerts
- Identify and contain device-based threats
- Hunt lateral movement on suspicious devices
- Proactively manage the attack surface

Ranger turns your SentinelOne protected endpoints into a distributed network of sensors that gives you visibility and control over the enterprise network attack surface. With Ranger you are now able to discover, identify, and contain any device-based threat in real time, and it enables you to autonomously protect compute infrastructure from IoT attacks, compromised devices, and vulnerabilities.

What's on your network?

Ranger creates visibility into your network by using distributed passive and active mapping techniques to discover running services, unmanaged endpoints, IoT devices, and mobile devices.

Network visibility. Ranger learns, maps, and reports what it sees on the network, enabling you to isolate unauthorized devices. Customizable scanning policies help avoid violating privacy statutes in an easy and transparent manner.

Network control. When unauthorized or compromised devices appear on the network, Ranger protects managed assets from unauthorized communications with one click.

No new software or hardware. Ranger does not require added hardware or network changes. The existing SentinelOne software intelligently elects which agents perform network scanning.

Ranger®

- Live global asset inventory
- Advanced ML device fingerprinting with flexible active + passive scanning
- Isolate suspicious and malicious devices
- Search in Deep Visibility™ from Ranger

How it blocks unknown devices

When an administrator chooses to block a device, that device is effectively isolated from all SentinelOne managed Windows, Mac, and Linux hosts. This is accomplished using local firewall rules as enforced by the SentinelOne agent on those devices.

What about employees on the road?

Can you prevent Ranger from scanning home, coffee shop, and other networks when employees are on the road? Absolutely. Ranger policies have several settings to maintain administrative control over what is and is not scanned. For example, you can set a minimum number of SentinelOne agents that must be on that network. If you set the number of SentinelOne agents at, say five, small home networks and coffee shops are unlikely to be scanned because you probably will never have five work computers on those networks at any one time. Further, administrators can require an explicit "yes, scan this network" from within the SentinelOne console to further control what is analyzed.

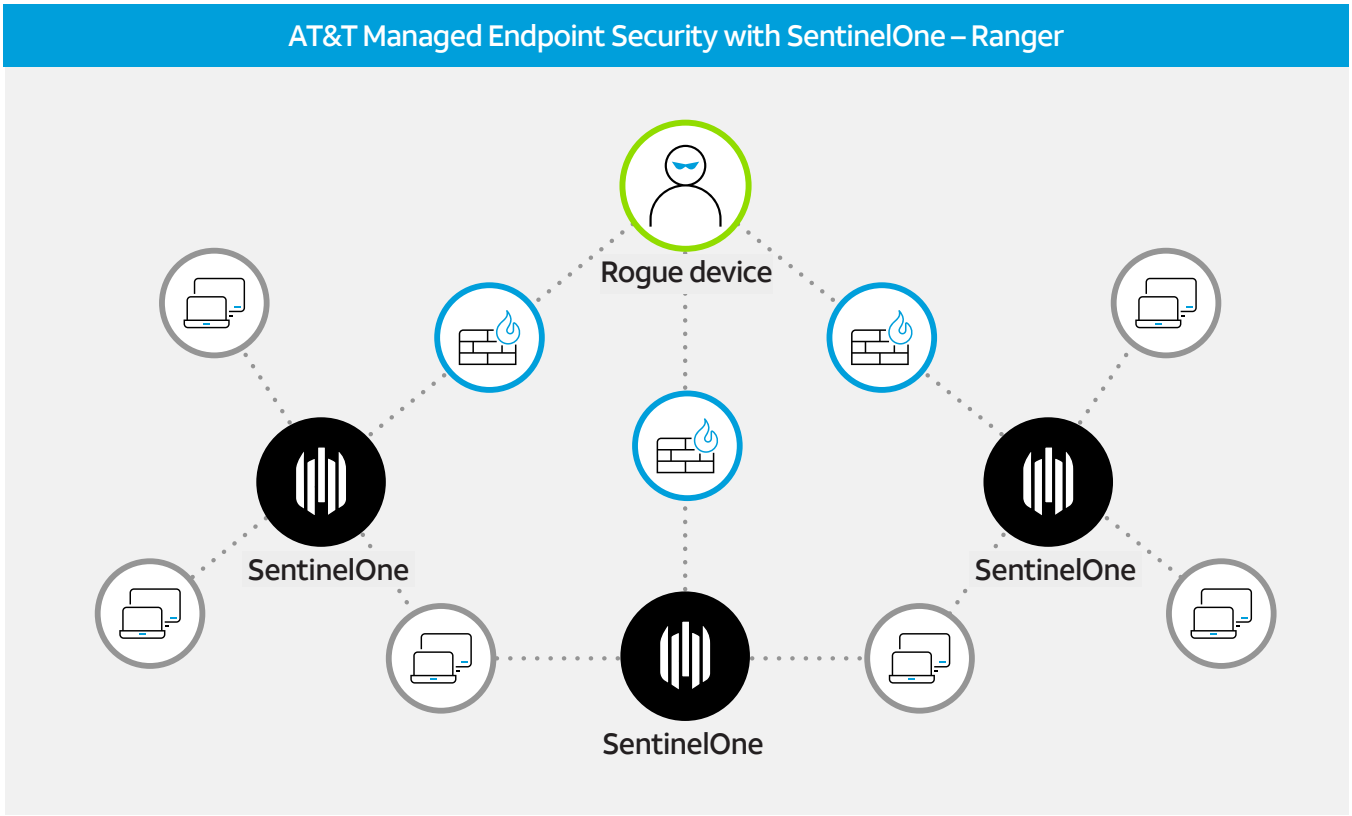
Managed security service benefits

AT&T Managed Endpoint Security with SentinelOne includes high-touch onboarding support and system setup, and 24/7 threat monitoring and management by the AT&T Security Operations Center (SOC). This helps alleviate the cybersecurity skill shortage, as well as the burden of daily operations and troubleshooting, at a cost that is often lower than hiring an in-house specialist.

It's easy to implement

- No network changes required. No network SPAN or TAP ports.
- Policies provide control over scan intervals, what should be scanned, and what must never be scanned.
- Choose between auto-enabled scanning or require explicit permission if more control is needed over the environment.

Forget about tedious manual traffic capture and upload for analysis. Ranger makes it automatic.



Get endpoint protection today.
Learn more at cybersecurity.att.com/products/sentinel-one

Why AT&T?

AT&T Cybersecurity helps reduce the complexity and cost of fighting cybercrime. Together, the power of the AT&T network, our Software-as-a-Service (SaaS)-based solutions, and our relationship with more than 40 best-of-breed vendors help accelerate your response to cybersecurity threats.

Contact your AT&T Business representative or learn more here.